Ingenix
Application Service Provider Privacy & Security Policies

Access	The Ingenix solution is a web-based, hosted solution and can be accessed from any computer with Internet access. All data is stored in the data center and no local software is required on the client system. All information that is transported from the data center to the client's browser is encrypted using the industry standard Verisign Secure Socket Layer 256-bit Encryption method. CareTracker has a robust internal security system that is based on Users and Roles. A User's setup and their respective Roles determine which applications and functions the user has access to. In addition, the role also determines whether the user has Read, Write, Edit, or Delete capability for any application. The CareTracker infrastructure is a highly available, fully redundant, fully load-balanced environment with many servers performing specific tasks simultaneously. The combination of this redundant server infrastructure with web-based connectivity means your data will always be available to you.
Authorization	CareTracker is hosted at Navisite which is a secure hosting facility. All equipment sits behind Cisco ASA firewalls with the only direct access through the web servers. CareTracker also includes the ability to allow access for users only from a specific IP Address.
Authentication	CareTracker has a robust internal security system that is based on Users and Roles. A User's setup and their respective Roles determine which applications and functions the user has access to. In addition, the role also determines whether the user has Read, Write, Edit or Delete capability for any application. Each operator has a single password that is used when the operator logs into the application. This login only occurs through a secure socket layer to CareTracker using Verisign for SSL encryption. The password is never transported in clear text and cannot be entered without the establishment of the secure connection. The password is stored after it is encrypted using a hashing algorithm. There are no reports, views, or any other mechanisms to display this password. Password controls are set up in CareTracker to force "strict" password usage which requires eight characters that include numbers, letters, a special character, and upper/lower case. In addition, password rules allow for setting password timeouts, password reuse, and password expiration timeframes to further control authentication. CareTracker's flexible security design allows you complete control over your users and you determine the level of access for each user.

Audit	CareTracker’s security model provides logging of all events that have occurred in the system. These events include user authentication and modifications as well as application events that have occurred. These logs provide a complete audit trail of what’s occurred on the system and can be viewed for a particular operator or for a particular patient. This allows you to always have all of the information you need for internal or external audits. The Navisite Data Center where CareTracker is audited annually with a SAS70 Type II report provided.
Secondary Uses of Data	At this time, Ingenix does not anticipate secondary uses for the data. All personal health information (PHI) will be used only in accordance with the obligations of our contract. In the event of any other use, Ingenix would use the data only under the terms of the master service agreement with each client and in accordance with all HIPAA requirements and applicable laws.
Data Ownership	Data is owned by the client. Per our standard Master Service Agreement, upon the termination of the relationship for any reason, at the client's request, Ingenix shall, at the client’s expense, turn over to the client (or its authorized agents or representatives) hard copies and/or magnetic media copies of all of the records, including but not limited to patient records, account files, doctors’ files, fee profile records, relevant third party communication and other data or files related in any way to the client’s business activities; provided, however, that Ingenix may retain one complete copy of client records or shall be given reasonable access to client records following termination of this Agreement for purposes of responding to billing inquiries and meeting any continuing or future legal obligations of Ingenix.